Osječki matematički list **6**(2006), 85–97

STUDENTSKA RUBRIKA

Eliptičke krivulje u kriptografiji

Dino Sejdinović*

Sažetak. U ovom članku definirali smo kriptosustav javnog ključa i ponovili njegovu povijest. Eliptička krivulja E nad proizvoljnim poljem je definirana i dana je geometrijska i algebarska interpretacija operacije uz koju E postaje Abelova grupa. Opisali smo upotrebu eliptičkih krivulja u kriptografiji kroz varijaciju ElGamalovog kriptosustava zasnovanog na algoritamskoj teškoći računanja diskretnog logaritma u konačnim grupama. Jednostavan primjer upotrebe kriptosustava eliptičkih krivulja (Menezes-Vanstone) je dan i opisane su prednosti ovog kriptosustava u odnosu na RSA/DES.

Ključne riječi: eliptičke krivulje, kriptografija javnog ključa, ElGamalov kriptosustav

Elliptical Curves in Cryptography

Abstract.
In this paper we define the public key cryptosystem and review its history. The elliptic curve E over a general field is defined and geometric and algebraic interpretation of the additive operation that makes E an abelian group is given. We describe the use of elliptic curves in cryptography through the variation of ElGamal Cryptosystem, based on the algorithmic difficulty of calculating a discrete logarithm in finite groups. A simple example of using the Elliptic Curve Cryptosystem (Menezes-Vanstone) is given and the advantages of this cryptosystem compared to RSA/DES are described.

Key words: elliptic curves, public key cryptography, ElGamal cryptosystem

1. Kriptosustavi sa javnim ključem

1.1. Potreba za javnim ključem

Ideju kriptosustava sa javnim ključem, tj. asimetričnog kriptosustava predložili su 1976. godine Whitfield Diffie i Martin Hellman. Naime, osnovni nedostatak klasičnih simetričnih kriptosustava je neophodnost da prije šifriranja pošiljalac i primalac (za koje su u kriptografskoj literaturi rezervirana imena Alice i Bob, a za njihovog protivnika Eve) najprije razmijene tajni ključ preko nekog sigurnog komunikacijskog kanala. Štoviše, bilo bi neophodno da oni često razmjenjuju ključeve,

*University of Bristol, Centre for Communications Research 1.31 Wireless & Networks Research Laboratory Merchant Venturers Building Department of Electrical & Electronic Engineering Bristol, BS8 1UB, UK, email: D.Sejdinovic@bristol.ac.uk

jer šifriranje više poruka istim ključem znatno smanjuje sigurnost. Osnovna ideja je onemogućiti protivnika (Eve) da, iako poznaje funkciju šifriranja e_K, izračuna funkciju dešifriranja d_K. Tada funkcija e_K može biti javna. Ulogu ovakvih funkcija šifriranja igraju tzv. osobne jednosmjerne funkcije (eng. *trapdoor one-way functions*). To su takve funkcije f koje je lako računati, a da je pritom f^{-1} vrlo teško (praktično nemoguće) izračunati osim u slučaju da je poznat neki dodatni podatak (eng. *trapdoor* – skriveni ulaz). Sada formalno možemo definirati kriptosustav sa javnim ključem:

Definicija 1. *Kriptosustav s javnim ključem je kriptosustav za čije familije funkcija šifriranja $\{e_K\}$, koje nazivamo javnim ključevima i funkcije dešifriranja $\{d_K\}$, koje nazivamo privatnim ključevima, pri čemu K prolazi skupom korisnika, vrijedi:*

(a) $\forall K \quad d_K = e_K^{-1}$,

(b) e_K *je javna funkcija, dok je* d_K *poznata samo korisniku* K,

(c) $\forall K$ e_K *je osobna jednosmjerna funkcija.*

1.2. Diffie-Hellmanov protokol za razmjenu ključeva

Diffie i Hellman su zapravo predložili protokol za razmjenu ključeva kroz javni komunikacijski kanal bez prethodnog razmjenjivanja bilo kakve informacije. To znači da je protivniku (Eve), iako zna sve podatke koji su prošli kroz javni komunikacijski kanal, nemoguće odrediti konačni tajni ključ. Pretpostavimo da su se Alice i Bob kroz javni komunikacijski kanal dogovorili o nekoj, jednostavnosti radi, cikličkoj i konačnoj grupi G koja ima $|G|$ elemenata i fiksirali njen generator g. Cilj im je da odrede jedan element grupe koji će biti ključ. Slijedi opis Diffie-Hellmanovog protokola koji objašnjava kako ovo uraditi.

Diffie-Hellmanov protokol

- Alice generira slučajan prirodan broj $a \in \{1, 2, \ldots, |G| - 1\}$ i pošalje Bobu element g^a.
- Bob generira slučajan prirodan broj $b \in \{1, 2, \ldots, |G| - 1\}$ i pošalje Alice element g^b.
- Alice izračuna $(g^b)^a = g^{ab}$.
- Bob izračuna $(g^a)^b = g^{ab}$. Sada je njihov tajni ključ $K = g^{ab}$.

Eve, koja prisluškuje komunikaciju, zna sljedeće podatke: G, g, g^a, g^b i potrebno je da iz ovih podataka izračuna g^{ab}. U tom slučaju kažemo da Eve rješava Diffie-Hellmanov problem (DHP). Ako ona može riješiti problem diskretnog logaritma (DLP) u grupi G, tj. iz podataka g i g^a izračunati a, onda može iz a i g^b naći i ključ $K = g^{ab}$. Vjeruje se da su za većinu grupa koje se koriste u kriptografiji problemi DHP i DLP ekvivalentni, tj. jedan na drugog svodivi u polinomijalnom vremenu. Također, u mnogim grupama DLP je algoritamski težak problem, pa za zgodnu osobnu jednosmjernu funkciju može poslužiti potenciranje u takvim grupama.

1.3. Razvoj kriptosustava sa javnim ključem

Iako su Diffie i Hellman predložili gore razmatrani formalni protokol šifriranja i dešifriranja pomoću javnog ključa zasnovan na težini logaritmiranja u konačnim grupama, oni nisu konstruirali i neki praktičan kriptosustav. Prvi kriptosustav sa javnim ključem predložili su 1978. godine R. L. Rivest, A. Shamir i L. M. Adleman koji po njima nosi naziv RSA kriptosustav. Sigurnost RSA se, umjesto na težini DLP problema, zasniva na težini problema faktorizacije cijelih brojeva, koji je po složenosti u mnogome sličan. Ovaj kriptosustav je trenutno u najširoj upotrebi. Zatim je 1985. godine Taher ElGamal predložio kriptosustav baziran na težini diskretnog logaritmiranja u multiplikativnoj grupi $\mathbb{Z}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ svih nenultih ostataka modulo p, gdje je p dovoljno velik prost broj, što je i bila ideja Diffie-Hellman protokola, a 1991. godine Schnorr je modificirao ElGamalov kriptosustav i učinio ga znatno efikasnijim. Na ElGamalovim tehnikama bazirana je i kriptografska tehnika *Digital Signature Algorithm* koju za vlastite potrebe koristi Vlada Sjedinjenih Američkih Država. Druga značajna primjena kriptosustava sa javnim ključem je *digitalni potpis*: kada Bob primi poruku $z = d_A(e_B(x))$, on može biti siguran da je poruku poslala Alice jer samo ona zna funkciju d_A.

Iste godine kada se pojavio ElGamalov kriptosustav, neovisno jedan od drugog, Neal Koblitz i Victor Miller su predložili kriptosustav eliptičkih krivulja, koji je također zasnovan na težini diskretnog logaritmiranja, ali sada na grupama točaka eliptičke krivulje.

2. Definicije i osnovne osobine eliptičkih krivulja

Definicija 2. *Neka je K polje karakteristike* $\operatorname{char} K \neq 2, 3$*, i neka je $x^3 + ax + b$, $a, b \in K$ polinom trećeg stupnja bez višestrukih korijena. Eliptička krivulja nad poljem K, u oznaci $E(K)$, je skup točaka (x, y), pri čemu su $x, y \in K$ i zadovoljavaju jednadžbu*

$$y^2 = x^3 + ax + b, \tag{1}$$

zajedno sa elementom označenim sa O, a koji nazivamo "točka u beskonačnosti".

Definicija 3. *Neka je K polje karakteristike* $\operatorname{char} K = 2$*. Eliptička krivulja nad poljem K je skup točaka (x, y), pri čemu su $x, y \in K$ i zadovoljavaju jednu od sljedećih jednadžbi:*

$$y^2 + cy = x^3 + ax + b, \tag{2}$$

ili

$$y^2 + xy = x^3 + ax^2 + b, \tag{3}$$

zajedno sa "točkom u beskonačnosti" O, pri čemu su $a, b, c \in K$ i polinomi na desnoj strani nisu nužno bez višestrukih korijena.

Definicija 4. *Neka je K polje karakteristike* $\operatorname{char} K = 3$*. Eliptička krivulja nad poljem K je skup točaka (x, y), pri čemu su $x, y \in K$ i zadovoljavaju jednadžbu*

$$y^2 = x^3 + ax^2 + bx + c, \tag{4}$$

zajedno sa "točkom u beskonačnosti" O, pri čemu su $a, b, c \in K$ i polinom na desnoj strani nema višestrukih korijena.

Opća jednadžba nad proizvoljnim poljem K:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5}$$

u slučaju da je $\operatorname{char} K \neq 2$ može biti transformirana u (4), a u slučaju da je $\operatorname{char} K > 3$ u (1). U slučaju polja karakteristike 2, (5) se transformira u jednu od jednadžbi (2) ili (3). Jednadžba (5) se još naziva Weierstrassovom formom, a s tim se u vezi (1) naziva skraćenom Weierstrassovom formom.

2.1. Eliptičke krivulje nad $\mathbb{R}$

U slučaju da je $K = \mathbb{R}$ polje realnih brojeva, eliptička krivulja $E(\mathbb{R})$, bez točke u beskonačnosti, se može prikazati kao krivulja u $\mathbb{R}^2$, tj. podskup ravnine. Promatrajmo ove krivulje kako bismo došli do centralnog rezultata teorije eliptičkih krivulja. Naime, skup točaka na eliptičkoj krivulji formira aditivnu Abelovu grupu, u odnosu na operaciju zbrajanja i koju ćemo kasnije definirati.

Definicija 5. *Neka je E eliptička krivulja nad poljem realnih brojeva $\mathbb{R}$ i P i Q dvije točke na E. Unarna prefiksna operacija $-$ na E je funkcija $- : E \to E$, koja ima sljedeća dva svojstva:*

(I_1) ako je $P = O$, onda je $-P = O$,

(I_2) ako je $P \neq O$, tj. $P = (x, y)$, pri čemu su $x, y \in \mathbb{R}$, onda je $-P = -(x, y) = (x, -y)$.

Iz definicije eliptičke krivulje, tj. iz jednadžbe (1) očigledno je da ako je $(x, y) \in E$, tada je i $(x, -y) \in E$.

Definicija 6. *Aditivna binarna operacija $+$ na E je funkcija $+ : E \times E \to E$, koja ima sljedeća četiri svojstva:*

(II_1) $\forall P \in E, \quad P + O = O + P = P$,

(II_2) $P + (-P) = O$,

(II_3) Ako P i Q imaju različite x koordinate, i pritom pravac l kroz točke P i Q nije tangenta na E, tada postoji pored P i Q još točno jedna točka presjeka pravca l sa E, označimo je sa R. Tada stavljamo:

$$P + Q = -R.$$

Ukoliko je pravac l kroz točke P i Q tangenta na E u P, odnosno Q tada stavljamo:

$$P + Q = -P, \text{ odnosno } P + Q = -Q.$$

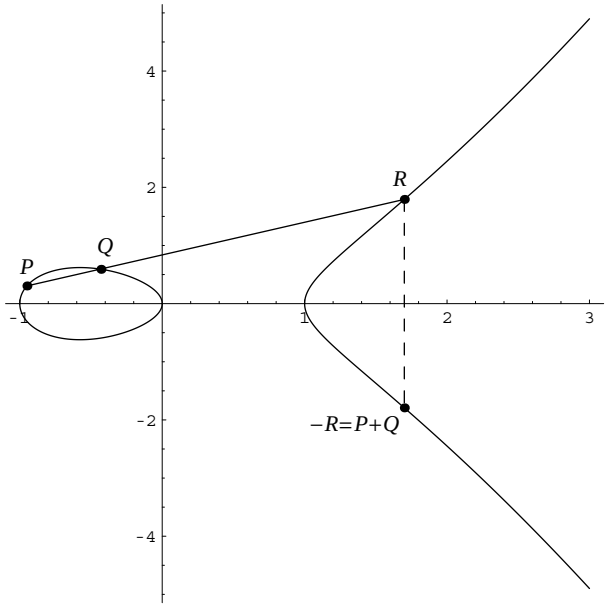
(II_4) Ako je $P = Q$, tada tangenta t na E u točki P, ako ima još i presjek R sa E, onda je taj presjek jedinstven. Tada stavljamo:

$$P + P = -R.$$

Ukoliko drugog presjeka nema (tada kažemo da t ima dvostruku tangenciju *u P, odnosno, da je P je točka inflekcije), onda stavljamo:*

$$P + P = -P.$$

Na ovaj način smo definirali operaciju "zbrajanja" nad skupom točaka eliptičke krivulje nad poljem realnih brojeva. Postoje razni načini da se pokaže da je eliptička krivulja nad poljem realnih brojeva $E(\mathbb{R})$, u odnosu na ovako definiranu operaciju zbrajanja, Abelova grupa. Sva svojstva Abelove grupe, osim asocijativnosti su gotovo evidentna. Najpoznatiji kompletni dokazi su zasnovani na projektivnoj geometriji ili na kompleksnoj analizi sa dvostruko periodičnim funkcijama. Pri tome, ulogu neutralnog elementa u grupi $(E(\mathbb{R}), +)$ igra točka u beskonačnosti O, dok je suprotni element točke P upravo točka $-P$. Mi se ovim dokazom nećemo baviti, već ćemo radije dati analitički izraz za zbrajanje na eliptičkoj krivulji i geometrijsku uvid u ovu operaciju.



Slika 1. Geometrijska interpretacija zbrajanja točaka eliptičke krivulje

Na slici 1 prikazano je "zbrajanje" na eliptičkoj krivulji. Konkretna je eliptička krivulja dana jednadžbom

$$E: \ y^2 = x^3 - x.$$

Ako su dane točke P i Q, najprije povučemo pravac l kroz P i Q, te pronađemo treću točku presjeka R pravca l sa krivuljom E. Rezultat zbrajanja je točka simetrična točki R u odnosu na x-os.

2.2. Eksplicitne formule zbrajanja na eliptičkim krivuljama

Analitički izraz za zbrajanje na eliptičkoj krivulji nad poljem realnih brojeva može se jednostavno izvesti.

Teorem 1. *Neka su $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke eliptičke krivulje $E(\mathbb{R})$ danoj s jednadžbom (1) i pri tome je $P \neq -Q$. Tada je $P + Q = (x_3, y_3)$, gdje su:*

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -y_1 + \lambda(x_1 - x_3),$$
$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{ako je } x_2 = x_1. \end{cases} \tag{6}$$

Dokaz. Neka je $x_2 \neq x_1$ i neka je jednadžba pravca l kroz točke P i Q dana sa $y = \lambda x + \mu$. Tada je očigledno:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ i } \mu = y_1 - \lambda x_1. \tag{7}$$

Točka pravca l leži na $E(\mathbb{R})$ ako i samo ako je $(\lambda x + \mu)^2 = x^3 + ax + b$. Dakle, za svaki korijen jednadžbe $x^3 - (\lambda x + \mu)^2 + ax + b = 0$ imamo x koordinatu jedne točke presjeka pravca l s krivuljom $E(\mathbb{R})$. Obzirom da već poznajemo dva korijena jednadžbe, a to su x_1 i x_2, na osnovu Vietéovih formula za jednadžbe trećeg stupnja je $x_3 = \lambda^2 - x_1 - x_2$. Naime, kako je $x^3 - (\lambda x + \mu)^2 + ax + b = (x - x_1)(x - x_2)(x - x_3)$, izjednačavajući koeficijente polinoma na lijevoj i desnoj strani (uz x^2) dobijamo da je $\lambda^2 = x_1 + x_2 + x_3$. Sada treća točka presjeka pravca l s krivuljom $E(\mathbb{R})$ ima koordinate $(x_3, \lambda x + \mu)$, što nam daje $P + Q = (x_3, -(\lambda x + \mu))$, pa nakon uvrštavanja relacija (7) dobijamo (6).

Slučaj $x_1 = x_2$, zbog $P \neq -Q$, zapravo znači $P = Q$. Tada je postupak sličan s tim što, umjesto određivanja koeficijenta smjera pravca kroz točke P i Q, određujemo koeficijent smjera tangente na krivulju danu jednadžbom (1) u točki P. Jednostavno, implicitnim deriviranjem jednadžbe (1) u točki P nalazimo da je $\lambda = (3x_1^2 + a)/2y_1$, odakle ponovno dobijamo (6). **Q.E.D.**

Dakle, operacija zbrajanja se najprije uvodi geometrijski, a zatim se određuju eksplicitne formule za koordinate zbroja točaka. Formule (6), uz ostala svojstva iz definicije zbrajanja, sada mogu poslužiti za definiciju zbrajanja na eliptičkim krivuljama $E(K)$ nad proizvoljnim poljem K, pri čemu je $\operatorname{char} K \neq 2, 3$, tj. za one eliptičke krivulje koje su definirane s (1). Analitički izrazi za zbrajanje na eliptičkoj krivulji nad poljima karakteristike 2 ili 3 su slični, uz male modifikacije.

Za primjene u kriptografiji najznačajnije su eliptičke krivulje nad konačnim poljima F_q s q elemenata, pri čemu su naročito zanimljivi slučajevi gdje je $q = p$ (prost broj) ili $q = 2^k$ potencija dvojke. S druge strane, u teoriji brojeva važnu ulogu igraju eliptičke krivulje nad poljem $\mathbb{Q}$ racionalnih brojeva. Najznačajniji rezultat teorije eliptičkih krivulja nad $\mathbb{Q}$ je Mordell-Weilov teorem koji kaže da je proizvoljna krivulja $E(\mathbb{Q})$ konačno generirana Abelova grupa, što znači da postoji konačan skup racionalnih točaka $P_1, P_2, \ldots, P_k$ u $E(\mathbb{Q})$ iz kojih se sve ostale racionalne točke na $E(\mathbb{Q})$ mogu dobiti povlačenjem tangenti i sekanti kroz prethodno izračunate točke.

2.3. Eliptičke krivulje nad konačnim poljem

Već smo rekli da su za primjene u kriptografiji najznačajnije eliptičke krivulje nad konačnim poljem F_q. U slučaju $q = p$ (prost broj) to su upravo polja $\mathbb{Z}_p$ ostataka

modulo p. Ukoliko je $q = p^k$ za neki prirodan broj k, onda postoji (do na izomorfizam) jedinstveno polje F_q čija je jedna od realizacija $\mathbb{Z}_p[x]/(f(x))$ gdje je $f(x)$ ireducibilni polinom stupnja k nad $\mathbb{Z}_p$. Elementi ovog polja su polinomi nad $\mathbb{Z}_p$ stupnja manjeg od ili jednakog od $k-1$, dok se zbrajanje i množenje naslijeđuju iz $\mathbb{Z}_p[x]$, s time što se nakon množenja računa ostatak pri dijeljenju dobijenog polinoma s polinomom $f(x)$. Da bi operacije u polju F_q, neophodne za računanje sa točkama na eliptičkoj krivulji nad ovim poljem, bile što jednostavnije, treba odabrati pogodan ireducibilan polinom $f(x)$. Pokazuje se da najbolje mogućnosti pružaju ireducibilni polinomi male težine, tj. oni polinomi koji imaju što manje nenultih koeficijenata.

Kriptosustavi eliptičkih krivulja uključuju i zgodan odabir povoljne eliptičke krivulje $E(K)$ nad nekim poljem K, kao i odabir povoljne *bazične točke* $P \in E(K)$. Kako bi saznali što više o strukturi grupe $E(K)$, a samim time napravili dobar izbor krivulje koju ćemo koristiti u našem kriptosustavu, korisno je znati točnu vrijednost reda grupe $E(K)$, kojeg ćemo označavati sa $\#E(K)$. Naravno, najzanimljiviji je slučaj konačnog polja $K = F_q$ koje ima q elemenata. Sljedeći teorem je jedan od najznačajnijih rezultata u vezi sa procjenom reda grupe $E(K)$.

Teorem 2. (Hasse) *Neka je F_q konačno polje s q elemenata i $E = E(F_q)$ eliptička krivulja nad F_q. Tada je*

$$|\#E - (q+1)| \leq 2\sqrt{q}. \tag{8}$$

Drugim riječima, za proizvoljnu eliptičku krivulju E nad F_q je $\#E = q + 1 - t$, pri čemu je $|t| \leq 2\sqrt{q}$. Broj $t = q + 1 - \#E$ naziva se *Frobeniusov trag* eliptičke krivulje E. Jasno, problem izračunavanja reda grupe E ekvivalentan je problemu izračunavanja Frobeniusovog traga eliptičke krivulje E. Također, na osnovu Frobeniusovog traga definiraju se takozvane anomalne i supersingularne krivulje.

Definicija 7. *Za eliptičku krivulju $E(F_q)$ nad konačnim poljem F_q kažemo da je* anomalna *ako je njen Frobeniusov trag $t = 1$, tj. ako je $\#E(F_q) = q$. Za eliptičku krivulju $E(F_q)$ nad konačnim poljem F_q, gdje je $q = p^k$, kažemo da je* supersingularna *ako karakteristika polja $p = \operatorname{char} F_q$ dijeli Frobeniusov trag t krivulje $E(F_q)$.*

Pokazalo se da se za kriptosustave formirane nad anomalnim i supersingularnim krivuljama mogu kreirati izuzetno efikasni napadi. Takav je MOV (Menezes-Okamoto-Vanstone) napad koji uspješno rješava problem diskretnog logaritma nad supersingularnom krivuljom. Stoga se u kriptografiji najčešće izbjegavaju anomalne i supersingularne krivulje i upravo zato je vrlo važno poznavati red grupe točaka eliptičke krivulje.

Jedan od najboljih načina da se točno izračuna $\#E$ je Schoofov algoritam (René Schoof, 1985). To je deterministički algoritam koji, za dano polje F_q i eliptičku krivulju E nad ovim poljem računa točnu vrijednost Frobeniusovog traga eliptičke krivulje E u $O(\ln^8 q)$ bitovnih operacija. Kasnije su Atkin i Elkies dali poboljšanu verziju Schoofovog algoritma s kompleksnošću $O(\ln^6 q)$, tako da je danas moguće izračunati $\#E(F_q)$ za sve $q < 10^{500}$. U detaljno razmatranje Schoofovog algoritma nećemo ulaziti, no njegova osnovna ideja zasniva se najprije na računanju ostataka $t_l = t \bmod l$, gdje su l svi prosti brojevi manji od l_{max}, pri čemu je l_{max} najmanji

prost broj za koji vrijedi

$$\prod_{\substack{2\leq l\leq l_{max}\\ l\text{ prost}}} l > 4\sqrt{q}, \tag{9}$$

nakon čega se iz određenih ostataka t_l, na osnovu kineskog teorema o ostacima, na jedinstven način može odrediti Frobeniusov trag t.

3. ElGamalov kriptosustav. Kriptosustav eliptičkih krivulja (ECC)

3.1. Problem diskretnog logaritma

Eliptičke krivulje su našle primjenu u kriptografiji kroz poopćenje ElGamalovog kriptosustava, koji je jedan od primjera kriptosustava sa javnim ključem. ElGamalov (Taher ElGamal, 1985) kriptosustav zasnovan je na neefikasnosti izračunavanja logaritama u nekim konačnim grupama. Naime, u radu sa realnim brojevima, potenciranje nije značajno lakša operacija od logaritmiranja, njoj inverzne operacije. No, u slučaju konačnih grupa, razlike su drastične. Metodom *square-and-multiply* jednostavno je naći bilo koju cjelobrojnu potenciju nekog fiksiranog elementa konačne grupe, ali je inverzna operacija, diskretni analogon logaritmiranju, koji ćemo i zvati diskretni logaritam, teška i kompliciran.

Definicija 8. *Neka je $(G,*)$ konačna grupa, $\alpha,\beta\in G$. Neka je i cijeli nenegativan broj. Stavimo $\alpha^0=e$, $\alpha^i=\alpha*\alpha*\ldots*\alpha$ (i puta). Neka je dalje:*

$$H=\langle\alpha\rangle=\{\alpha^i : i\geq 0\}$$

ciklička grupa generirana elementom α. Problem diskretnog logaritma (DLP) sastoji se u nalaženju jedinstvenog cijelog broja m, gdje je $0\leq m\leq |H|-1$, da bude $\alpha^m=\beta$. Ukoliko ovakav broj postoji on se naziva diskretnim logaritmom i označava s $m=\log_\alpha\beta$.

3.2. ElGamalov kriptosustav

Originalno, kriptosustav koji je predložio ElGamal koristio je multiplikativnu grupu $G=\mathbb{Z}_p^*=(\mathbb{Z}/p\mathbb{Z})^*$ svih nenultih ostataka modulo p, pri čemu je α bio primitivni korijen modulo p, odnosno generator grupe $\mathbb{Z}_p^*$, a p dovoljno velik prost broj. U ovom slučaju je uz oznake prethodne definicije $G=H$. Najbrži poznati algoritmi za traženje diskretnog logaritma u $\mathbb{Z}_p^*$ zahtijevaju broj operacija reda $\exp(O((\log p)^{1/3}(\log\log p)^{2/3}))$, što znači da je problem diskretnog logaritma po kompleksnosti ekvivalentan problemu faktorizacije.

Primjer 1. *Neka je $G=\mathbb{Z}_{19}^*$. Diskretni logaritam od 7 po bazi 2 je 6, jer je $2^6\equiv 7(\mathrm{mod}19)$.*

ElGamalov kriptosustav

- Neka je p prost broj i $\alpha\in\mathbb{Z}_p^*$ primitivni korijen modulo p. Vrijednosti p i α su javne. Svaki korisnik sistema K odabire svoj tajni ključ $a_K\in\mathbb{Z}_{p-1}^*$ i obznanjuje vrijednost $\beta_K=\alpha^{a_K}(\,\mathrm{mod}\,p)$.

- Alice šalje Bobu tajnu poruku $x \in \mathbb{Z}_p^*$ tako što odabere slučajni broj $k \in \mathbb{Z}_{p-1}$ i proslijeđuje javnu poruku

$$e_B(x,k) = (y_1, y_2) = (\alpha^k \bmod p, x\beta_B^k \bmod p).$$

- Bob sada računa:

$$d_B(y_1,y_2) = y_2(y_1^{a_B})^{-1} \bmod p = x(\alpha^{a_B})^k((\alpha^k)^{a_B})^{-1} \bmod p = x \bmod p = x,$$

gdje je a_B njegov tajni ključ.

Na neki način, suština ElGamalovog kriptosustava leži u množenju poruke x sa "maskom" β^k. Onaj koji poznaje tajni eksponent a može jednostavno iz α^k naći β^k, invertirati ga i tako ukloniti "masku".

Primjer 2. *Neka su se Alice i Bob dogovorili (javno) da koriste grupu* $\mathbb{Z}_{31}^*$ *i fiksirali element* $\alpha = 3$ *ove grupe. Alice odabire svoj tajni ključ* $a_K = 7$*, dok Bob odabire tajni ključ* $a_B = 22$*. Sada Alice šalje Bobu element* $\beta_A = 17 (= 3^7 \bmod 31)$*, a Bob odgovara s* $\beta_B = 14 (= 3^{22} \bmod 31)$*.*

Alice Bobu želi proslijediti tajnu informaciju $x = 24$*, odabire neki slučajan broj* k*, recimo* $k = 5$ *i računa:* $y_1 = 3^5 \bmod 31 = 26$ *i* $y_2 = 24 \cdot 14^5 \bmod 31 = 27$*. Bob sada prima brojeve* 26 *i* 27 *i računa:* $27 \cdot (26^{22})^{-1} \bmod 31 = 27 \cdot 5^{-1} \bmod 31 = 27 \cdot 25 \bmod 31 = 24$*. I tako je Bob sigurno primio informaciju* $x = 24$*.*

Primijetimo da Bobu ni u kom slučaju nije potrebno da zna slučajni broj $k = 5$ *niti Alicein tajni ključ* $a_A = 7$*.*

3.3. Kriptosustav eliptičkih krivulja

ElGamalov kriptosustav sada jednostavno možemo modificirati da umjesto grupe $\mathbb{Z}_p^*$ koristi grupu eliptičke krivulje nad konačnim poljem, npr. grupu $E(\mathbb{Z}_p)$. Naime, definicija problema diskretnog logaritma vrijedi i u ovim grupama i, štoviše, razlika u težini problema potenciranja i logaritmiranja još je veća. Naravno, ovdje treba voditi računa o tome da je eliptička krivulja aditivna, a ne multiplikativna Abelova grupa, pa zapravo "potenciranje" točke na eliptičkoj krivulji predstavlja njeno uzastopno zbrajanje sa samom sobom, ili, uvjetno rečeno, množenje skalarom (prirodnim brojem). Isto vrijedi i za problem "logaritmiranja" - treba naći takav prirodan broj k za koji je $k \times P = P + P + \ldots + P$ (k puta) $= Q$, gdje su P i Q date točke eliptičke krivulje.

Točka $k \times P \in E(\mathbb{Z}_p)$, za danu točku P i prirodan broj k, jednostavno se pronalazi algoritmom *double-and-add* (udvostruči i dodaj), koji je analogon algoritmu *square-and-multiply* za pronalaženje k-te potencije nekog elementa. Ovaj jednostavni, ali vrlo korisni algoritam zahtijeva $O(\log k \log^3 p)$ bitovnih operacija i koristi binarni zapis broja $k = k_0 + k_1 2 + \ldots + k_{m-1}2^{m-1}$. Idući kroz petlju veličine m točka P se uzastopno udvostručuje (zbraja sa samom sobom) i pri i-toj iteraciji dobijena vrijednost se dodaje varijabli u koju želimo smjestiti konačan rezultat samo kada je $k_i = 1$. Tako, primjerice, točku $100P = 64P + 32P + 4P = 2^6P + 2^5P + 2^2P$ možemo odrediti pomoću svega 6 udvostručavanja i 2 zbrajanja točaka na krivulji.

Analogon ElGamalovog kriptosustava koji koristi eliptičke krivulje nad $\mathbb{Z}_p$

- Dano je polje $\mathbb{Z}_p$ s p (prost broj) elemenata, eliptička krivulja $E = E(\mathbb{Z}_p)$ i bazična točka $P \in E$ i svi ovi podaci su fiksirani i javni. Svaki korisnik sistema K odabire proizvoljan prirodan broj a_K – njegov tajni ključ, a zatim izračuna i obznani točku $Q_K = a_K \times P$.

- Alice šalje Bobu tajnu poruku P_m – neka točka eliptičke krivulje E, koja za Boba znači određenu informaciju, tako što odabere slučajni prirodan broj k i proslijeđuje javnu poruku

$$e_B(P_m, k) = (C_1, C_2) = (k \times P, P_m + k \times Q_B).$$

- Bob sada računa:

$$d_B(C_1, C_2) = C_2 - a_B \times C_1 = P_m + k \times (a_B \times P) - a_B \times (k \times P) = P_m.$$

No, pokazalo se da doslovno prevođenje ElGamalovog kriptosustava na eliptičke krivulje ima i određenih nedostataka. Prvi je, što se iz gore predloženog kriptosustava da i naslutiti, taj što prije šifriranja moramo elemente otvorenog teksta prevesti (uroniti) u točke na eliptičkoj krivulji, za što i ne postoji odgovarajući deterministički algoritam. U ovakvim slučajevima koriste se probabilistički algoritmi koji u slučaju da je eliptička krivulja dana sa jednadžbom (1), pronalaze takve x za koje je $x^3 + ax + b$ kvadrat modulo p. Naime, ako su jedinice otvorenog teksta cijeli brojevi između 0 i M, za jedinicu m tražimo takav $x = mk + j$, gdje je k broj pokušaja a $j \in \{1, 2, \ldots, k\}$ minimalan da bude x^3+ax+b kvadrat modulo p. Nakon izračunavanja y za koje vrijedi (1), jedinici otvorenog teksta m pridružujemo točku $(x, y) \in E$. Pokazuje se da je približna vjerojatnost da iz k pokušaja pronađemo približna vjerojatnost da iz k pokušaja pronađemo broj x, dana s $1-(1/2)^k$. Dakle, već za $k > 30$ imamo sasvim zadovoljavajuću vjerojatnost, ali ostaje činjenica da determinističkog algoritma nema.

Nadalje, nedostatak je i taj da se poruka šifriranjem čak učetverostruči – umjesto jednog cijelog broja, dobijamo uređeni par točaka eliptičke krivulje. Stoga su predložene i druge varijante kriptosustava eliptičkih krivulja. Takav je i sljedeći, Menezes-Vanstoneov kriptosustav, kod kojeg je prosljeđena poruka, umjesto četverostruko, dvostruko veća od originalne poruke. Kod ovog kriptosustava, umjesto prevođenja jedinice otvorenog teksta u točku eliptičke krivulje, na izvjestan način, imamo samo "maskiranje" jedinice otvorenog teksta alatima koje pružaju eliptičke krivulje. Dakle, nema nikakve potrebe za kompliciranim (i nesigurnim) postupkom prevođenja otvorenog teksta na jezik točaka eliptičke krivulje.

Menezes-Vanstoneov kriptosustav eliptičkih krivulja

- Dano je polje $\mathbb{Z}_p$ s $p > 3$ (prost broj) elemenata, eliptička krivulja $E = E(\mathbb{Z}_p)$, bazična točka $P \in E$, H ciklička podgrupa grupe E generirana točkom P i svi ovi podaci su fiksirani i javni. Svaki korisnik sistema K odabire proizvoljan prirodan broj a_K – njegov tajni ključ, a zatim izračuna i obznani točku $Q_K = a_K \times P$

- Alice šalje Bobu tajnu poruku $M = (x_1, x_2) \in \mathbb{Z}_p^* \times Z_P^*$, dakle ne nužno točku na eliptičkoj krivulji E, tako što odabere proizvoljno $k \in \mathbb{Z}_{|H|}$i proslijeđuje poruku

$$e_B(x_1, x_2, k) = (C, y_1, y_2) = (k \times P, c_1 x_1 \bmod p, c_2 x_2 \bmod p),$$

pri čemu je $(c_1, c_2) = k \times Q_B = k \times (a_B \times B)$.

- Bob sada računa: $a_B \times C = (c_1, c_2)$, a zatim i

$$d_B(C, y_1, y_2) = (y_1 c_1^{-1} \bmod p, y_2 c_2^{-1} \bmod p) = (x_1, x_2).$$

Primjer 3. *Neka su Alice i Bob odabrali krivulju E definiranu s $y^2 = x^3 + x + 1$ nad poljem $\mathbb{Z}_{31}$. Javna bazična točka je $P = (9, 10)$. Može se pokazati da je $\#\mathbb{Z}_{31} = 34$ i da je P točka reda 34. Stoga je $H = \mathbb{Z}_{31}$. Sve točke eliptičke krivulje E mogu se prikazati sljedećom tablicom:*

k	$k \times P$	k	$k \times P$	k	$k \times P$	k	$k \times P$	k	$k \times P$	k	$k \times P$
1	$(9, 10)$	7	$(6, 24)$	13	$(27, 10)$	19	$(5, 22)$	25	$(16, 23)$	31	$(23, 13)$
2	$(18, 29)$	8	$(24, 29)$	14	$(26, 21)$	20	$(26, 10)$	26	$(24, 2)$	32	$(18, 2)$
3	$(23, 19)$	9	$(16, 8)$	15	$(5, 9)$	21	$(27, 21)$	27	$(6, 7)$	33	$(9, 21)$
4	$(4, 22)$	10	$(20, 2)$	16	$(19, 3)$	22	$(28, 18)$	28	$(17, 13)$	34	O
5	$(25, 16)$	11	$(22, 22)$	17	$(10, 0)$	23	$(22, 9)$	29	$(25, 15)$		
6	$(17, 18)$	12	$(28, 13)$	18	$(19, 28)$	24	$(20, 29)$	30	$(4, 9)$		

Prostor otvorenih tekstova je sada $\mathbb{Z}_{31}^* \times \mathbb{Z}_{31}^*$, odakle uviđamo još jednu prednost Menezes-Vanstoneovog kriptosustava. Naime, broj otvorenih tekstova koje možemo šifrirati je znatno veći. Poruke koje se na ovaj način proslijeđuju možemo poistovjetiti sa uređenim parovima alfabetskih znakova. Primjerice, ako koristimo engleski alfabet možemo poistovjetiti "a" s 1, "b" s 2,..., "z" s 26. Sada komunikacija između Alice i Boba može teći na sljedeći način:

- Alice odabire tajni ključ 7 i obznanjuje točku $7 \times P = (6, 24)$ izračunatu *double-and-add* algoritmom

- Bob odabire tajni ključ 12 i obznanjuje točku $12 \times P = (28, 13)$ izračunatu *double-and-add* algoritmom

- Alice Bobu želi poslati poruku "ok", tj. $(x_1, x_2) = (15, 11)$. Odabire slučajan broj $k = 5$. Nakon što izračuna $(c_1, c_2) = 5 \times (28, 13) = (24, 29)$, $5 \times P = (25, 16)$ te $c_1 x_1 = 24 \cdot 15 \bmod 31 = 19$ i $c_2 x_2 = 29 \cdot 11 \bmod 31 = 9$, šalje poruku $((25, 16), 19, 9)$.

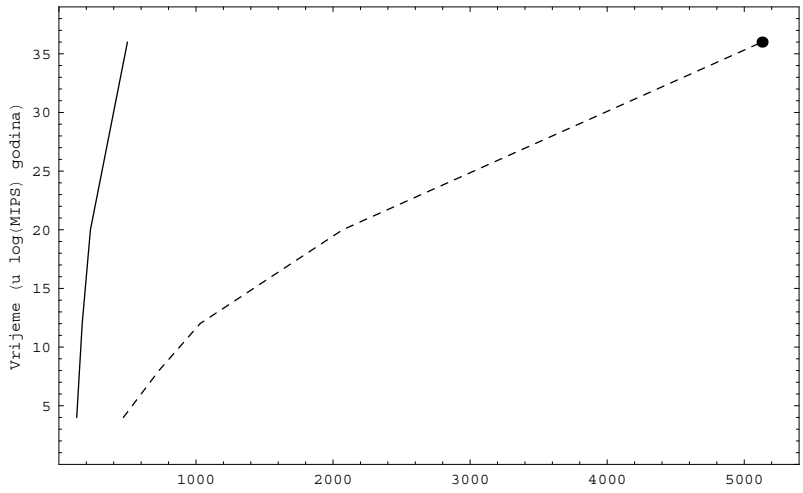
- Nakon što primi ovu poruku, Bob najprije nađe $(c_1, c_2) = 22 \times (25, 16) = (24, 29)$, zatim invertira elemente 24 i 29 modulo 31 koristeći prošireni Euklidov algoritam: $24^{-1} \bmod 31 = 22$ i $29^{-1} \bmod 31 = 15$. Sada Bob može očitati originalnu poruku kao: $(19 \cdot 22 \bmod 31, 9 \cdot 15 \bmod 31) = (15, 11)$, tj. "ok".

4. Sigurnost kriptosustava eliptičkih krivulja

Kriptosustav eliptičkih krivulja (ECC – *Elliptic Curve Cryptosystem*) je kriptosustav javnog ključa koji postaje predmet velikog interesa kriptografa. Dok je do 2003.

godine najveći faktorizirani RSA modul imao 530 bita, a najveći riješeni problem diskretnog logaritma u ElGamalovom kriptosustavu 397 bita, najveći riješeni problem diskretnog logaritma na eliptičkim krivuljama u ECC kriptosustavu imao je svega 109 bita. Grafikon na slici 2 pokazuje usporedbu sigurnosti ECC i RSA/DSA kriptosustava u ovisnosti od veličine ključa. Mjeru sigurnosti predstavlja vrijeme potrebno za razbijanje ključa najefikasnijim poznatim algoritmima izraženo u MIPS godinama. MIPS godina je uobičajena mjera sigurnosti kriptosustava i ona zapravo predstavlja broj operacija izvršenih tijekom jedne godine na računalu koje izvršava milijun instrukcija svake sekunde. Opće je prihvaćeno da 10^{12} MIPS godina potrebnih za otkrivanje ključa implicira da je dani kriptosustav po današnjim standardima siguran. Za ovakvu sigurnost RSA/DSA kriptosustavi zahtjevaju modul od 1024 bita, dok je za ECC dovoljan modul sa 160 bita. Ova razlika povećavanjem veličine ključa postaje još izrazitija. Na primjer, ECC sa 300-bitnim modulom osigurava istu sigurnost kao i RSA/DSA sa 2000-bitnim modulom.

Zbog svega navedenog, jasno je da kriptosustavi eliptičkih krivulja postaju sve interesantnija opcija, pogotovo u primjenama kod kojih je u dizajnu sistema važan kriterij memorija – takvi su, primjerice, smart kartice i mobilni telefoni.



Slika 2. Usporedba sigurnosti ECC (puna linija) i RSA/DSA (isprekidana linija) kriptosustava

Literatura

[1] A. DUJELLA, *Teorija brojeva u kriptografiji*, PMF - Matematički odjel, Sveučilište u Zagrebu, Poslijediplomski kolegij, 2003

[2] N. KOBLITZ, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics 114, Springer-Verlag, New York, 1994

[3] M. MARETIĆ, *Eliptičke krivulje u kriptografiji*, Diplomski rad, PMF - Matematički Odjel, Sveučilište u Zagrebu, 2002

[4] M. Saeki, *Elliptic Curve Cryptosystems*, M. Sc. thesis, School of Computer Science, McGill University, Montreal, 1997

[5] N. Torii, K.Yokoyama, *Elliptic Curve Cryptosystem*, Fujitsu Sci. Tech. J., 36/2 , pp.140-146 (2000)